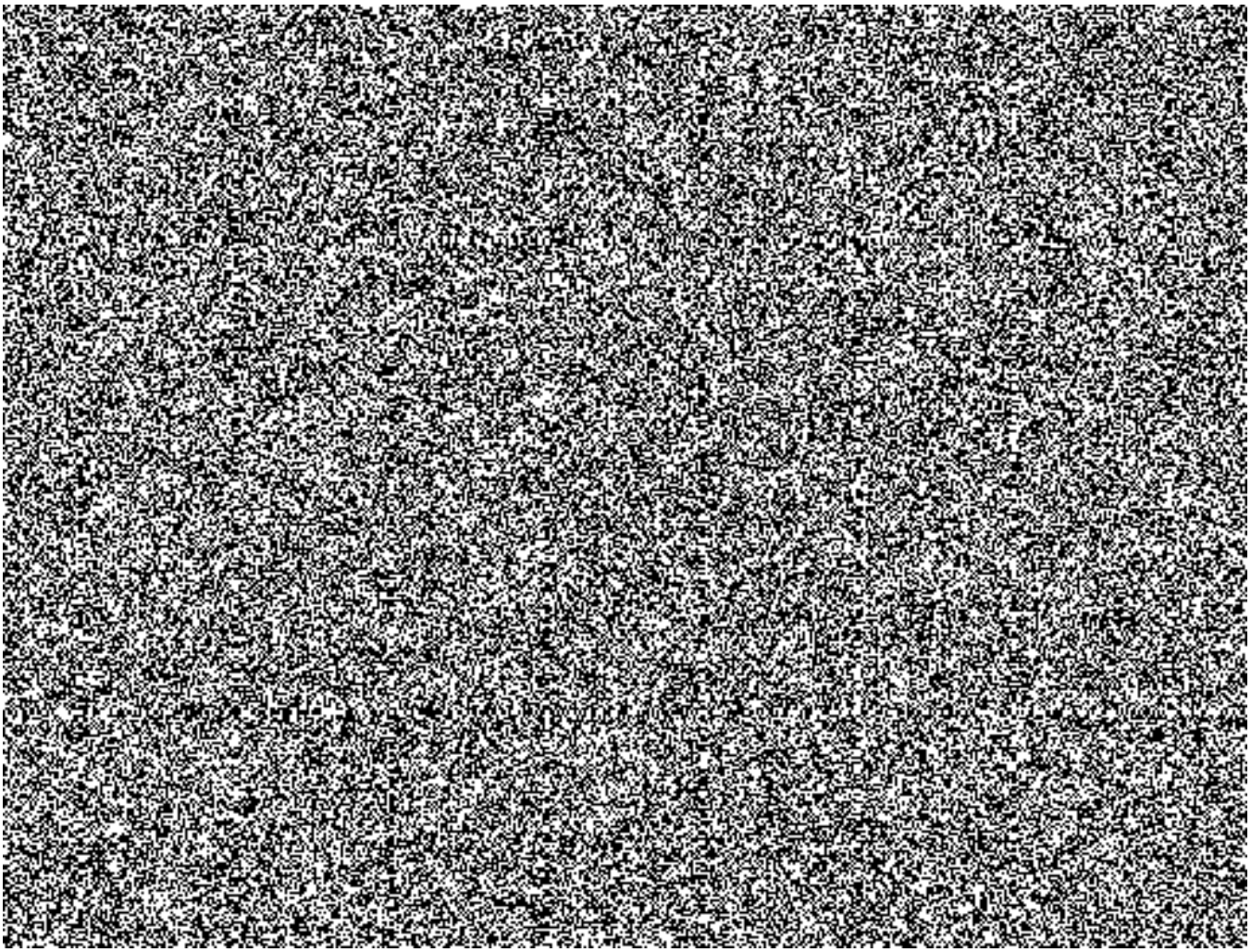
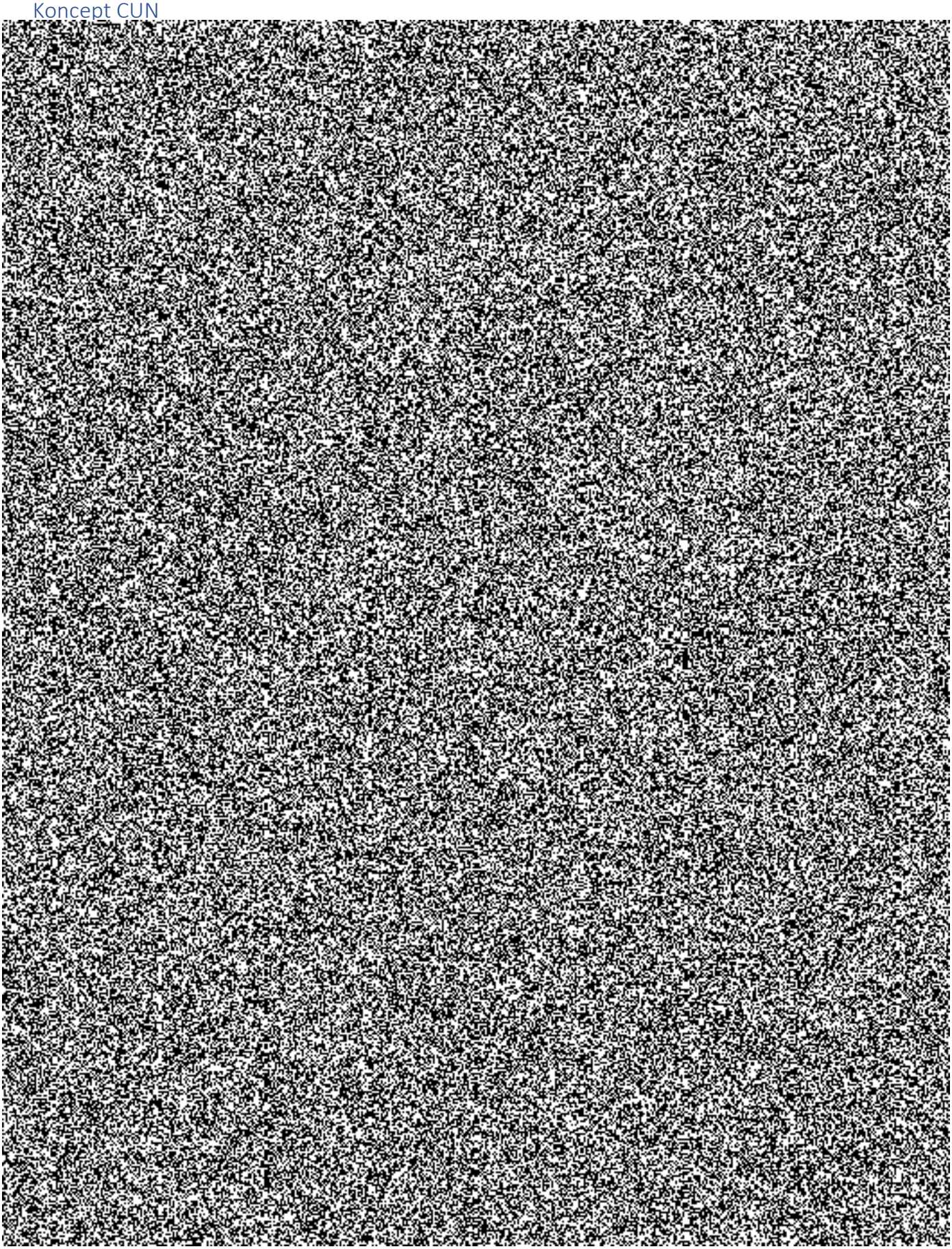
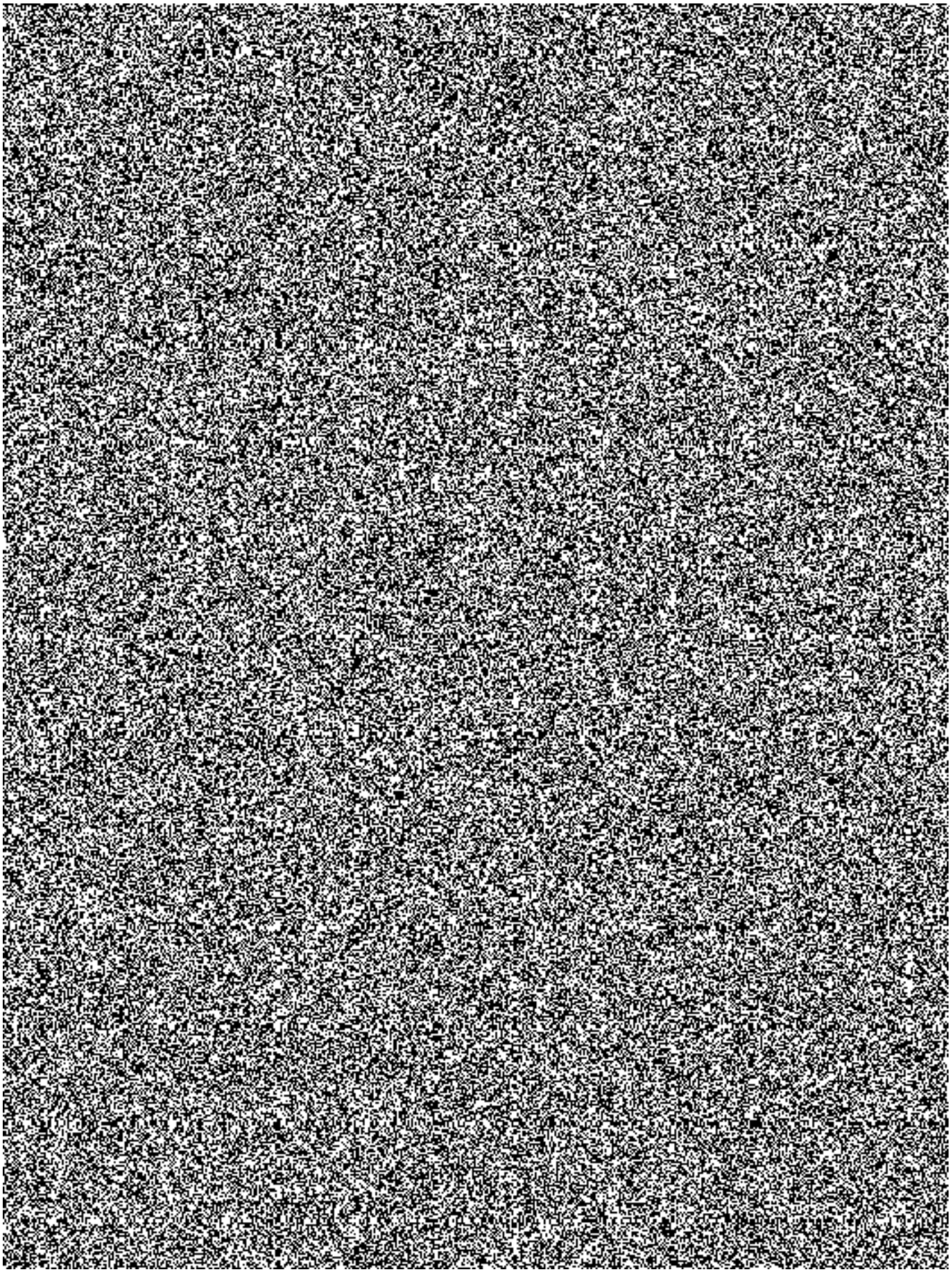
Příloha č. 1

Technická specifikace Díla

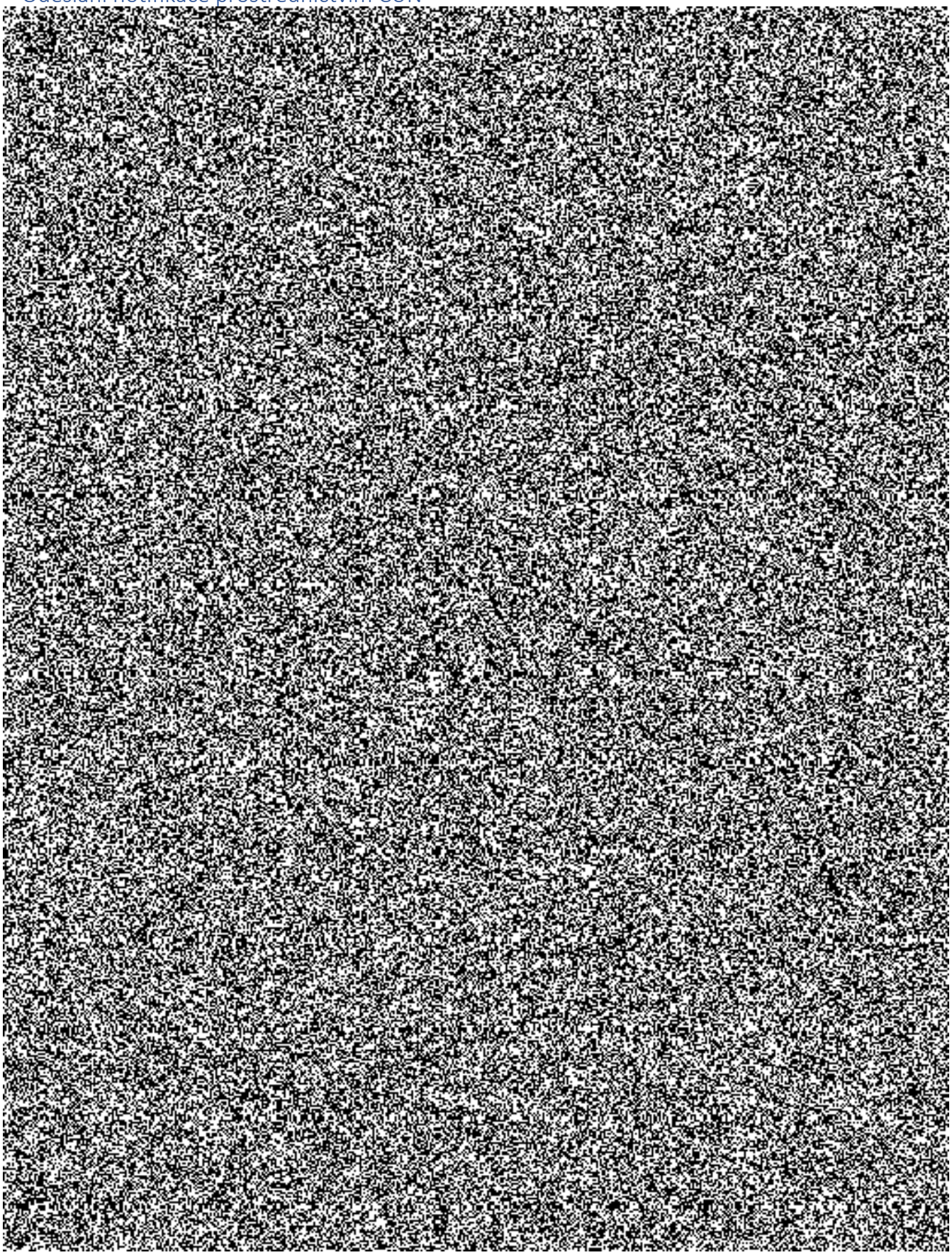
1. Centrální uživatelské notifikace

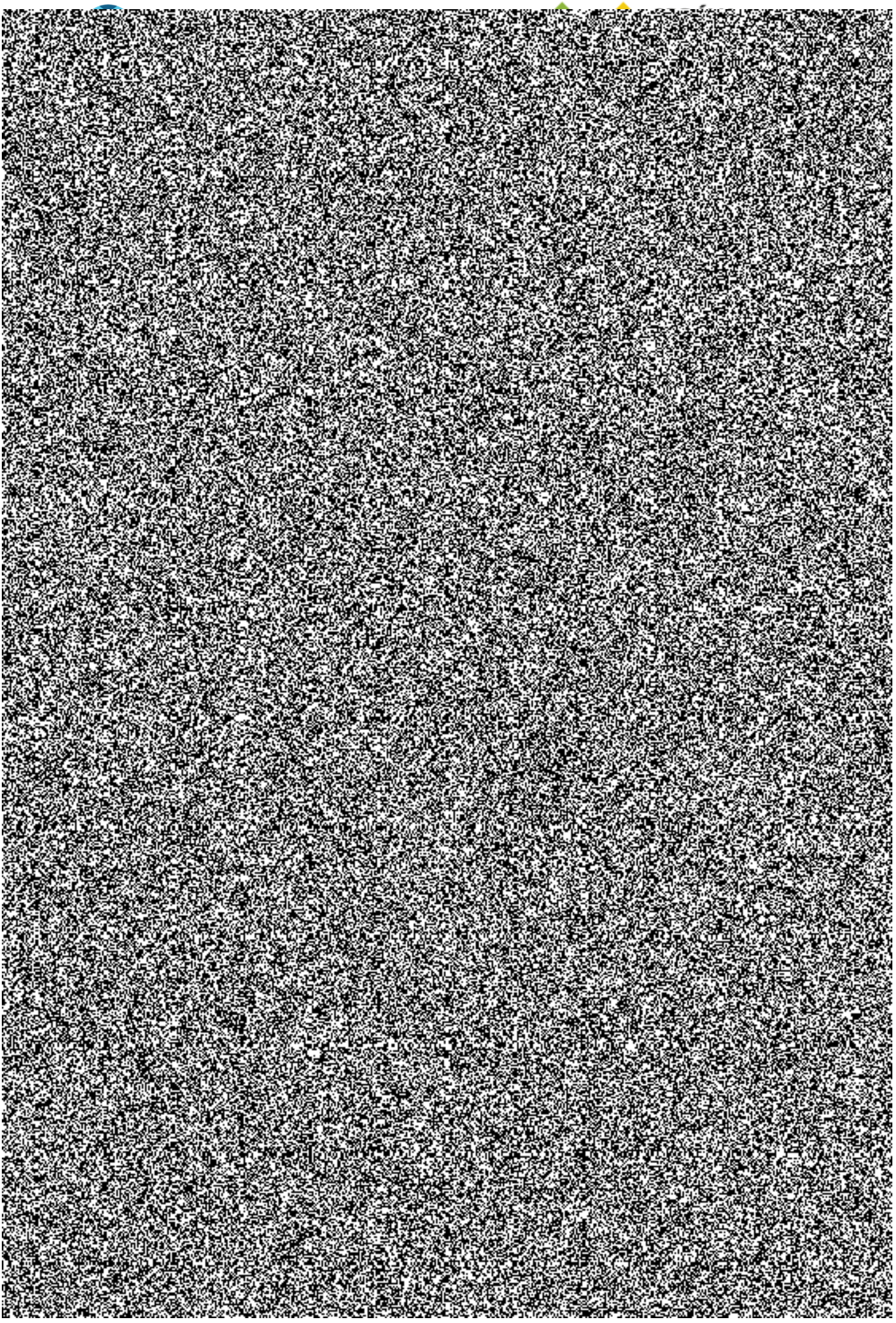


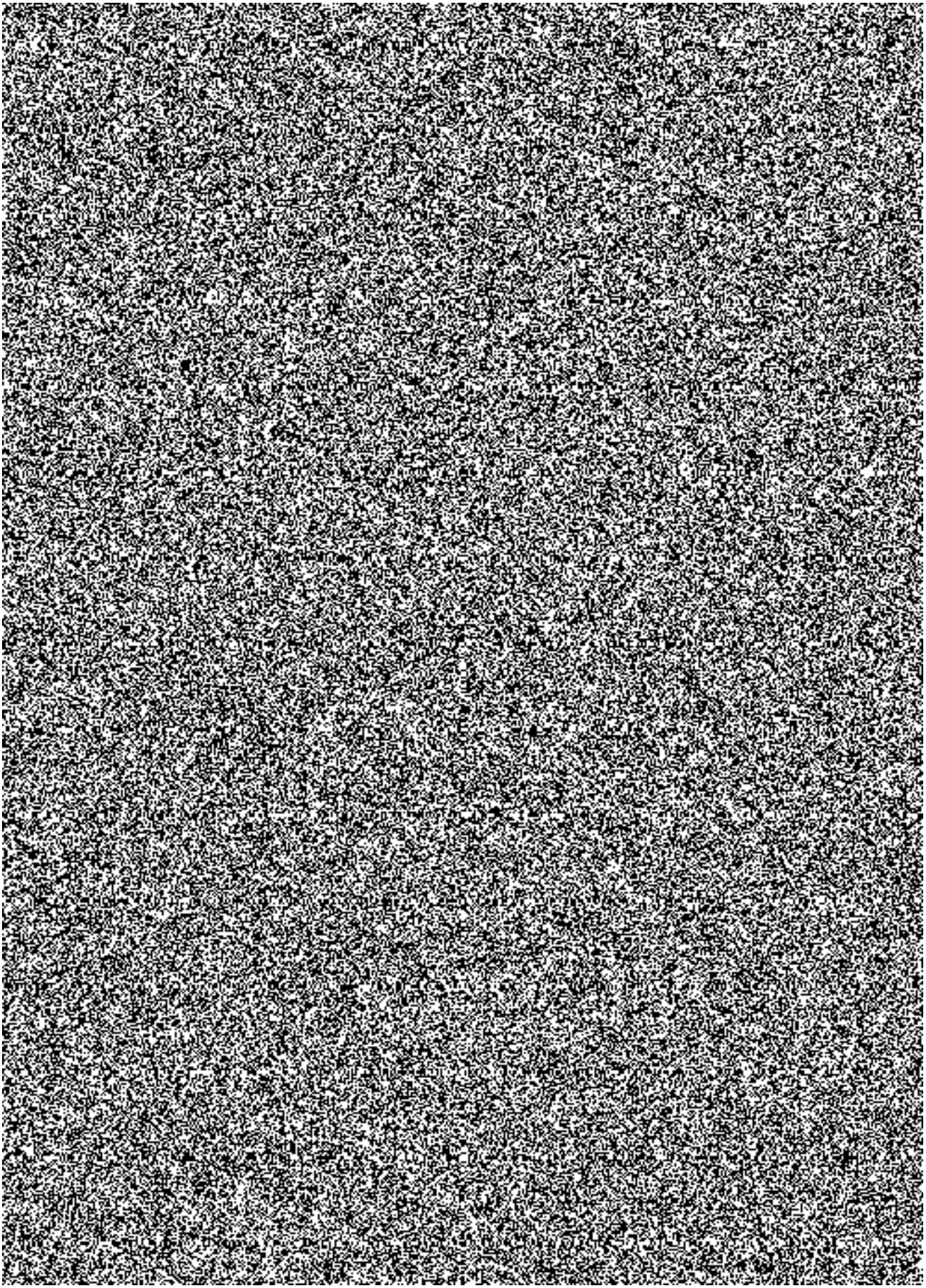


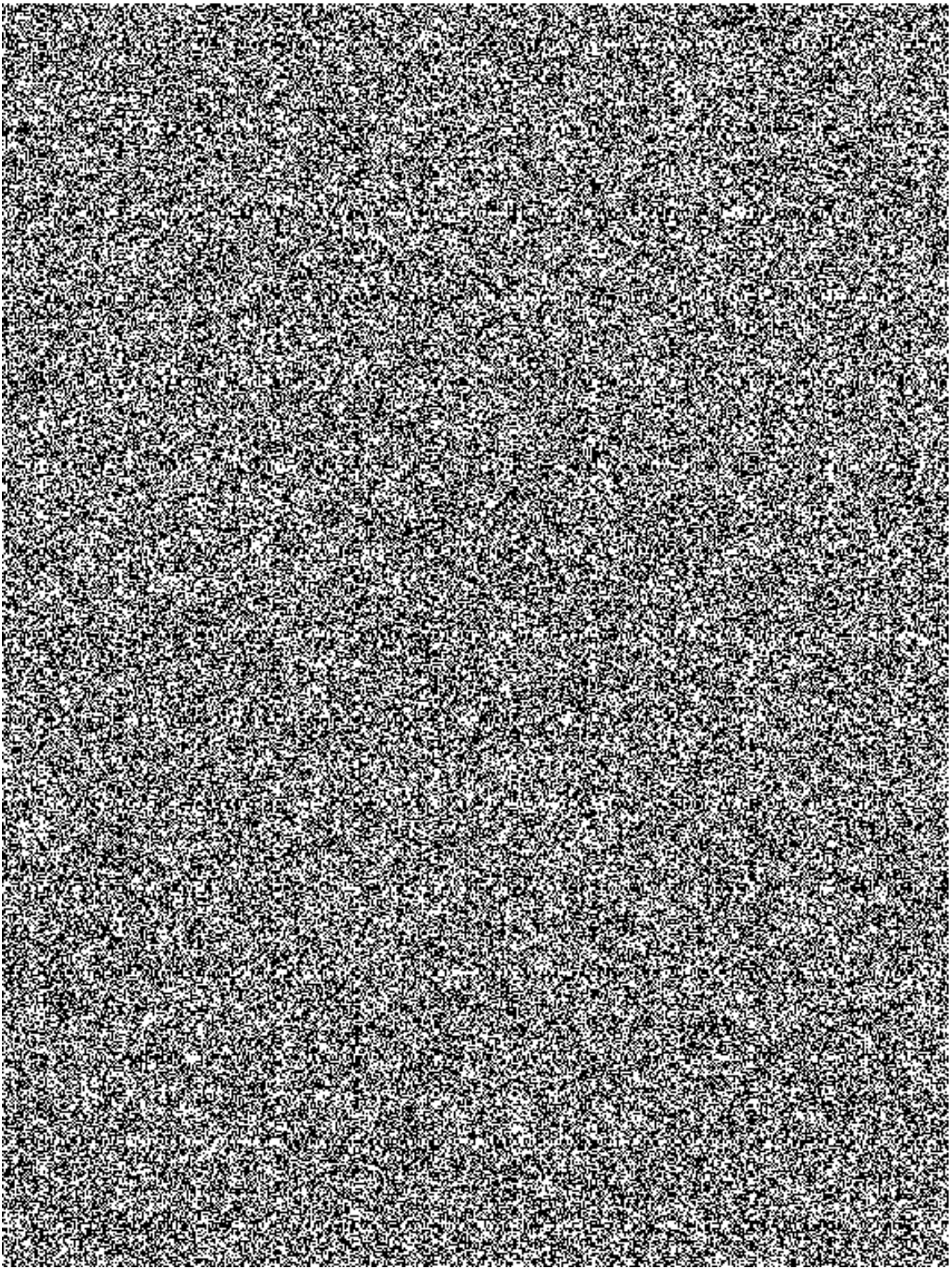


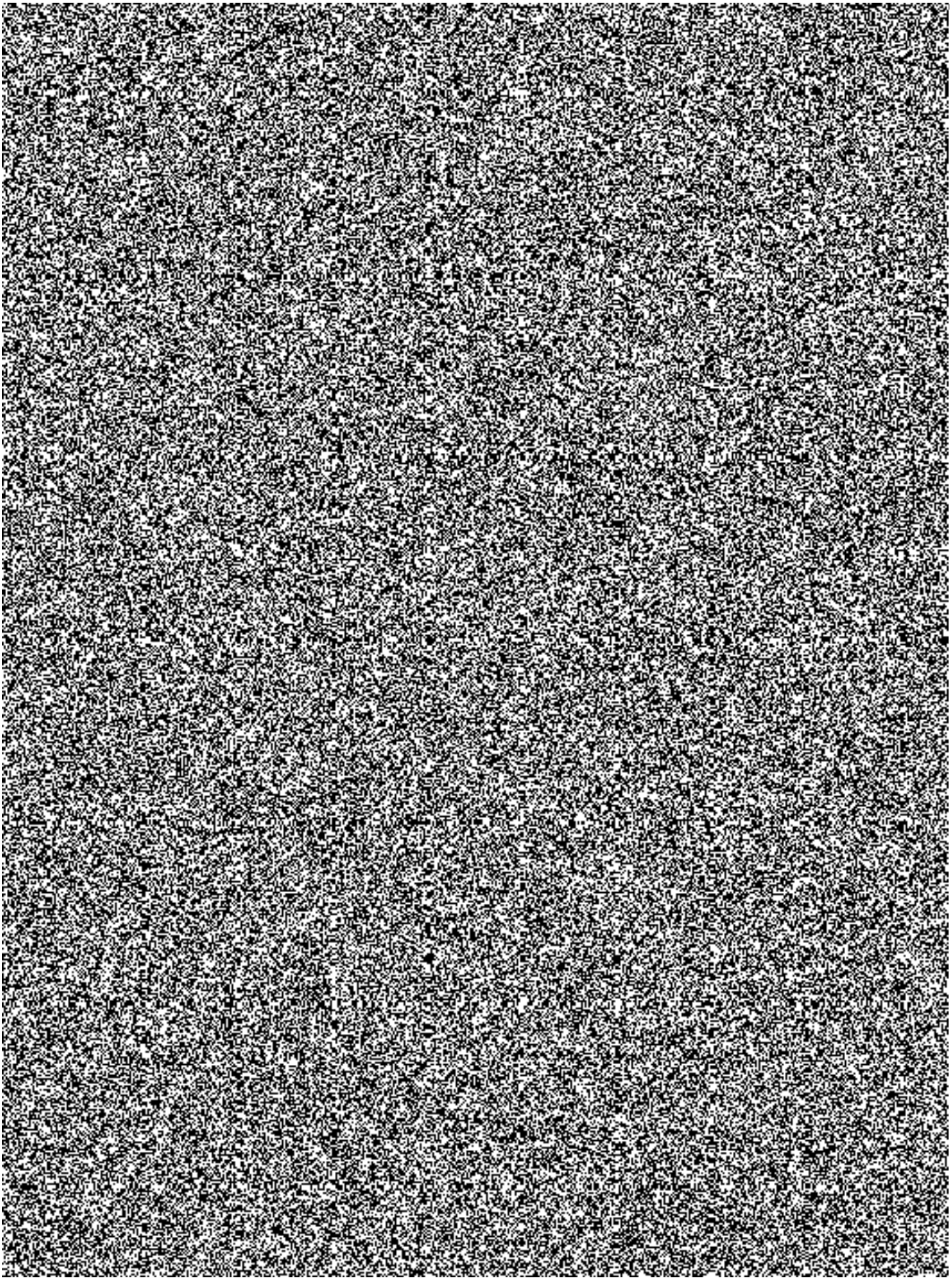
Odeslání notifikace prostřednictvím CUN

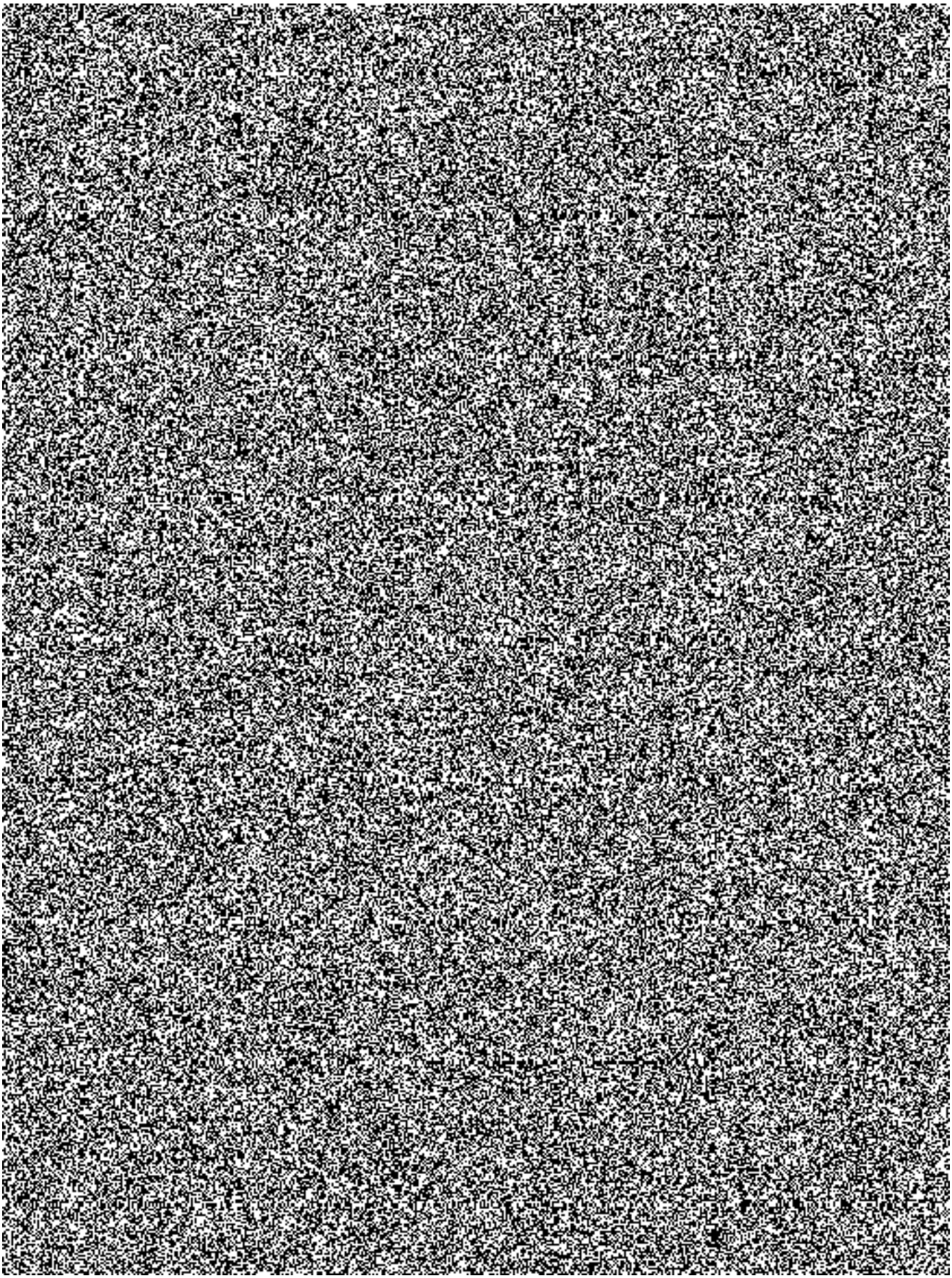












Nefunkční požadavky

Modul	Parametr	Požadovaný výkon (doba odezvy)/ throughput [Tx/s]
CUN	Doba odezvy na každou jednotlivou službu	< 1000 ms / 10 transakcí (volání služeb) za sekundu 90% volání

2. Notifikace po změně údaje u UPS

Na základě úspěšné změny kontaktního údaje k IdP UPS (telefonní číslo nebo e-mailová adresa) na portálu národního bodu bude na původní kontakt zaslána informativní zpráva o provedené změně.

3. Povinný certifikát jen na produkci

V rámci konfigurace kvalifikovaného poskytovatele v prostředí TEST nebude načtení veřejné části šifrovacího certifikátu povinné.

4. Nasazení (1x nasazení release na produkci)

Kompletní nasazení nových funkcionalit na produkční prostředí. Smoke a regresní testy po nasazení na prostředí, které ověří správnou funkčnost aplikace.

5. Školení (proškolení SD SZR před nasazením release)

Proškolení SD SZR před nasazením nového release v rozsahu změn, které se v rámci release budou nasazovat, včetně dodání změnové dokumentace ke školení.

6. Penetrační test (vč. ceny třetí strany)

Budou provedeny externí penetrační testy, které budou zaměřeny na vybrané komponenty řešení MORIS dostupné z veřejné sítě Internet. Toto testování bude zaměřeno na ověření funkčnosti aplikačního celku NIA. Cílem penetračního testu bude odhalit co největší množství závažných zranitelností na úrovni konektorů služeb systému, na úrovni referenčních infrastrukturních prvků, ve webovém rozhraní aplikace a prostředí, na kterém aplikace běží, odhalit způsob jejich využití a případnou možnost získání přístupu.

Plán testů – postup a způsob realizace:

- Proběhnou penetrační testy bez znalosti prostředí (black box) a s částečnou znalostí prostředí (grey box – zejm. v případě webových služeb), kdy proběhne simulace počínání útočníků ve výše popsaných rolích / scénářích.
- Externí dodavatel předá zástupcům NAKIT výsledky provedených testů v podobě stručného dokumentu, ve kterém bude uveden soupis nálezů, indikace jejich závažnosti a technické

detaily potřebné pro odstranění nálezů. O kritických zjištěních budou zástupci NAKIT informování neprodleně telefonicky.

- Po vypořádání nálezů menšího rozsahu proběhne opětovné otestování (retest) za účelem ověření účinnosti aplikovaných nápravných opatření. Poté bude vyhotoven návrh závěrečné zprávy dle standardů externího dodavatele, které vyhovují požadavkům NAKIT. V závěrečné zprávě budou k jednotlivým zjištěním doplněny výsledky opakovaného testu.

7. Seznam zkratek

AIFO	Agendový identifikátor fyzické osoby
AIS	Agendový informační systém
ASCII	American Standard Code for Information Interchange („americký standardní kód pro výměnu informací“)
BSI	Bezvýznamový směrový identifikátor
CUL	Centrální uživatelské logování
CUN	Centrální uživatelské notifikace
FCM	firebase Cloud Messaging
IČO	Identifikační číslo osoby
ID	Identifikátor
IdP	Poskytovatel identity
iOS	Mobilní operační systém
ISZR	Informační systém základních registrů
MEP	Mobilní elektronický prostředek
MK	Mobilní klíč
MORIS	Modulární registr pro informační systémy
NAKIT	Národní agentura pro komunikační a informační technologie
NB	Národní bod
NIA	Národní identitní autorita
ORG	Převodník identifikátorů
PBSI	Převodník bezvýznamových směrových identifikátorů
ProfileID	Identifikátor profilu v národním bodu
ROB	Registr obyvatel
RPP	Registr práv a povinností
SD	Service Desk.
SDÚ	Subjektem definované údaje
SeP	Poskytovatel služeb
SMS	Služba krátkých textových zpráv
SMTP	Simple Mail Transfer Protocol – Internetový protokol určený pro přenos zpráv elektronické pošty
SZR	Správa základních registrů
UPS	Username, password, SMS
UTF8	UCS/Unicode Transformation Format. Je to způsob kódování řetězců znaků Unicode/ISO/IEC 10646 do sekvencí bajtů.